Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

Bis 1. April 2021 zu erfüllende Anforderungen samt Praxishinweisen

Anlage 1: Anforderungen für <u>Praxen</u>

Software: Rechner-Programme, Mobile Apps und Internet-Anwendungen

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
1	Mobile Anwendungen (Apps)	Sichere Apps nutzen	Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps restlos löschen.	Apps nur aus vertrauenswürdigen Hersteller-App-Stores installieren (z.B. "App Store", "Google Play Store" oder „Microsoft Store“). Für Android-Geräte: In den Sicherheitseinstellungen keine Apps aus externen Quellen zulassen.
2	Mobile Anwendungen (Apps)	Aktuelle App-Versionen	Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.	„Automatische Updates“ Funktion unterstützt bei einer zeitnahen Installation aktueller App-Versionen
4	Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Keine vertraulichen Daten über Apps versenden.	Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden, muss der Datenversand entsprechend eingeschränkt werden (z.B. über die Einstellungen der App). Wenn möglich vor der App-Benutzung prüfen ob ungeschützte Protokollierungs- oder Hilfsdateien geschrieben werden, die vertrauliche Informationen preisgeben.
5	Office-Produkte	Verzicht auf Cloud-Speicherung	Keine Nutzung der in Office-Produkte integrierte Cloud-Speicher zur Speicherung personenbezogener Informationen.	Vertrauliche Daten könnten über Cloud-Speicherung ungewollt veröffentlicht werden. Bei der Auswahl und Installation von Office-Produkten z.B. beachten: - Office 365/OneDrive möglichst nicht verwenden - Office 2013: „Microsoft SkyDrive Pro“ deaktivieren.
6	Office-Produkte	Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten	Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.	Entfernen der Metadaten wie "Autor(en)" und "zuletzt geändert von" aus Office-Dokumenten, unter „Datei“ → „Eigenschaften“. Verwendung von Funktionen zur automatisierten Prüfung auf Restinformationen oder Warnung vor vorhandenen Restinformationen.

7	Internet-Anwendungen	Authentisierung bei Webanwendungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.	Achten Sie auf sichere 2-Faktor-Authentisierung oder verwenden Sie hinreichend komplexe Passwörter (vgl. Anlage 1 - Anforderung Nr. 34) oder Passwortmanager mit generierten Passwörtern. Achten Sie auf verschlüsselte Verbindungen (vgl. Anlage 1 - Anforderung Nr. 10).
8	Internet-Anwendungen	Schutz vertraulicher Daten	Stellen Sie Ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.	Im Browser die Einstellungen zu Cookies, Verlauf und Formulardaten anpassen. Diese können auch jedes Mal manuell gelöscht werden: - Chrome, Firefox, Edge: "Strg" + "Umschalt" + "Entf" - Safari: "cmd" + "alt" + "E". Alternativ Browser wie "Firefox Klar" verwenden, die diese Daten mit einem Klick oder nach Beendigung der Anwendung automatisch löschen.
10	Internet-Anwendungen	Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.	Nur http**s**://... Webseiten nutzen und ggf. Erweiterungen/ Add-Ons verwenden, die eine Verschlüsselung sicherstellen (z.B. HTTPS Everywhere). https Webseiten werden durch ein "Schloss" als Icon im Webbrowser visualisiert. Durch Anklicken des Schlosses lassen sich die Informationen zu dem Zertifikat und dem Herausgeber des Zertifikats einsehen.

Hardware: Endgeräte und IT-Systeme

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
12	Endgeräte	Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras	Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.	Mikrofon- oder Kameradeaktivierung (abhängig vom Gerät) über: - entsprechende Softwarefunktionen - Entzug von Zugriffsberechtigungen - physische Abdeckung, Ausschaltung oder Trennung. Bei der Anschaffung neuer Geräte sollte darauf geachtet werden, dass die Kamera abgedeckt und das Mikrofon ausgeschaltet werden kann. Eine Diode weist meist auf die aktive Benutzung der Geräte hin, und bietet einen Indikator für missbräuchliche Nutzung.
13	Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.	Unbeaufsichtigte Geräte sperren: - Windows-Rechner: Windows-Taste + L - Mobile Geräte: Sperrtaste

15	Endgeräte	Einsatz von Viren-Schutzprogrammen	Setzen Sie aktuelle Virenschutzprogramme ein.	Verwenden Sie "Windows Defender" oder ein kommerzielles Virenschutzprogramm. Konfigurieren Sie, welche Daten wann gescannt werden sollen (z. B. alle Dateien vor dem Schreiben, eingehende E-Mail, etc.). Ein aktuell gehaltener Virenscanner für Geräte sollte: - Dateizugriffe prüfen, um die Ausführung schadhafter Dateien zu verhindern - versendete und empfangene Dateien prüfen, um die Ausführung schadhafter Dateien zu verhindern - den gesamten Datenbestand regelmäßig prüfen, um vergangene Infektionen mittels neuer Signaturen zu finden - Änderungen am Virenscanner von Benutzern (z.B. Deinstallation oder Konfigurationsänderungen) verhindern
19	Smartphone und Tablet	Schutz vor Phishing und Schadprogrammen im Browser	Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.	Alle (mobilen) Endgeräte sollten vor Schadprogrammen geschützt werden. Im verwendeten Browser sollte die Funktion „Safe Browsing“ bzw. die Funktion zur Warnung vor schädlichen Inhalten von Browsern aktiviert werden. Schutz durch achtsamen Umgang mit Zugangsdaten: - Überprüfen der URL, auf der die Zugangsdaten eingegeben werden - Misstrauen gegenüber E-Mails mit einem Link und der Aufforderung, Zugangsdaten dort einzugeben - Nutzung von Browser-Lesezeichen / Bookmarks, um auf der korrekten Webseite zu landen.
20	Smartphone und Tablet	Verwendung der SIM-Karten-PIN	SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.	Schutz der SIM-Karte durch eine PIN. Nutzung von Super-PIN/PUK durch einen festgelegten Prozess und Verantwortlichen schützen.
22	Smartphone und Tablet	Verwendung eines Zugriffschutzes	Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.	Komplexe Gerätesperrcodes anstatt einfache Mustersperren nutzen. Bildschirmsperre nutzen und angemessen kurze, automatische Bildschirmsperre aktivieren. Vertrauliche Informationen nicht auf dem Sperrbildschirm anzeigen. Nach mehreren fehlgeschlagenen Entsperrversuchen sollte sich das mobile Gerät in den Werkszustand

				zurücksetzen und dabei vertrauliche Daten und Verschlüsselungsschlüssel sicher vernichten.
23	Smartphone und Tablet	Updates von Betriebssystem und Apps	Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.	„Automatische Updates“-Funktion unterstützt bei der Installation aktueller App-Versionen. Betriebssystem-Updates werden in der Regel über eine entsprechende Benachrichtigung auf dem Gerät angekündigt.
27	Mobiltelefon	Updates von Mobiltelefonen	Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.	Ein Backup hilft Ihnen bei einem fehlgeschlagenen Update. Überprüfen Sie, ob nach den Updates ungewünschte Einstellungen wie die automatisierte Nutzung von Cloud-Speichern aktiviert wurden.
29	Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.	Datenträgerkennzeichnungen könnte erfolgen durch: - Liste, die eine Kennzeichnung eines Datenträgers eindeutig zuordenbar macht - zwischen Sender und Empfänger abgestimmte Systematik, die für Dritte keine Rückschlüsse ermöglicht (z.B. Datenträger: "dd2bbeab-d901-4043-b543" statt "Onkologischer Befund Patient XY".
30	Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Versand-Anbieter mit sicherem Nachweis-System, Manipulationssichere Versandart und Verpackung.	Nutzung eines abgesicherten Versands einer oder mehrerer Postunternehmen. Über die Angebote der sicheren Nachweissysteme wie Einschreiben und Wertsendungen informiert Sie Ihr Postunternehmen.
32	Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.	Es wird dringend empfohlen eine Hardware-Firewall einzusetzen und diese nach den eigenen Anforderungen zu konfigurieren und zu warten. Nur erlaubte Kommunikationsziele (IP-Adressen und Ports) und -protokolle zulassen (eingehend/ausgehend). Besonders sensible Systeme innerhalb des Praxisnetzes isolieren.
33	Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.	Dokumentation der logischen Struktur des Netzes (insbesondere Subnetze, Zonen und Segmente). Änderungen im Netzwerk sollten dokumentiert werden.

Anlage 2: Zusätzliche Anforderungen für <u>mittlere Praxen</u>

Software: Rechner-Programme, Mobile Apps und Internet-Anwendungen

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
1	Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Minimierung der App-Berechtigungen.	Bevor eine App in einer Institution eingeführt wird, muss sichergestellt werden, dass nur für die Funktionen benötigte Berechtigungen erlaubt sind. Weitere Berechtigungen hinterfragen und gegebenenfalls unterbinden. Sicherheitsrelevante Berechtigungseinstellungen müssen so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können. Wo dies technisch nicht möglich ist, müssen die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.

Anlage 3: Zusätzliche Anforderungen für <u>Großpraxen</u>

Hardware: Endgeräte und IT-Systeme

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
10	Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.	Sichere und nicht veraltete Verschlüsselungsverfahren einsetzen. Empfehlungen zu geeigneten Algorithmen und Schlüssellängen bieten die Technischen Richtlinien des BSI „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1). Mittels Open-Source Lösungen wie VeraCrypt können entsprechende verschlüsselte Container angelegt werden.

Anlage 5: Anforderungen für <u>dezentrale Komponenten der Telematikinfrastruktur</u>
<u>Achtung: Geltung bereits ab 1. Januar 2021</u>

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
5	Dezentrale Komponenten der TI	Geschützte Kommunikation mit dem Konnektor	Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.	Clients sind die mit dem TI-Konnektor verbundenen Systeme, z.B. Kartenterminals und Praxisverwaltungssysteme (PVS). Geeignete Schutzmaßnahmen sind z.B.: - Aktivierung der verschlüsselten TLS-Verbindung vom PVS zum Konnektor - Aktivierung der Authentisierungsmöglichkeit am Konnektor. Für die Authentisierung mittels X.509 Clientauthentisierung muss ein Zertifikat im Konnektor generiert und das PVS inklusive PIN und Zugriff auf den privaten Schlüssel konfiguriert, oder ein Konnektor-fremdes X.509 Zertifikat muss im PVS inklusive PIN und Zugriff auf den privaten Schlüssel und im Konnektor konfiguriert werden.